**Listing of the Claims**

This listing of claims will replace all prior versions, and listings, of claims in the application.

***Claims***

1-9. Canceled

10. (Previously Presented) A method for transferring a first super-root key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first super root key using a second super-root key of the key provider system;

b) providing within the second other system a first secure module having third and fourth super-root keys within a memory circuit thereof, the third and fourth super-root keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted root keys and encrypted super-root keys and for storing the decrypted keys within a memory circuit of the first secure module, and wherein the third and fourth super-root keys are other than accessible outside of the module, and wherein the third and fourth super-root keys are private keys;

b1) automatically generating by the first secure module a super-root key request in dependence on a super-root key status;

c) transferring the encrypted first super-root key from the key provider system to the second other system via the information network in response to the super-root key request;

d) providing the encrypted fourth super-root key to the processor internal to the first secure module of the second other system; and,

e) executing program code on the processor internal to the first secure module to decrypt the encrypted first super-root key using the third super-root key stored within the memory circuit of the first secure module and to store the decrypted first super-root key internally within a secure key memory location of the first secure module.

11. (Previously Presented) A method for transferring a first super-root key between a key provider system and a second other system via an information network according to claim 10 further comprising the steps of:

f) executing program code on the processor internal to the first secure module to store the decrypted first super-root key within the memory circuit of the first secure module at a location corresponding approximately to the location where the fourth super-root key was stored.

12. (Previously Presented) The method according to claim 11 wherein one of the third and fourth super-root keys are only replaceable through use of the other of the third and fourth super-root keys.

13. Canceled

14. (Previously Presented) The method according to claim 11 wherein the step of storing the decrypted first super-root key comprises the steps of:

i1) erasing the fourth super-root key from a first storage area of the memory circuit; and,

i2) storing the decrypted first super-root key within approximately the same first storage area of the same memory circuit.

15-20. Canceled

21. (Previously Presented) A secure module for use in a system for transferring a secure super-root key between a key provider system and a second other system via an information network that is other than secure, the secure module in operative communication with the second other system, the secure module including:

an encryption processor;

an input port for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor;

a memory circuit in operative communication with the encryption processor for storing a first super-root key within a first memory location thereof and for storing a second super-root key within a second other memory location thereof;

memory storage having program code stored therein and executable on the encryption processor for, upon receipt of an encrypted third super-root key, decrypting the encrypted third super-root key using one of the first and second super-root keys and for storing the decrypted third super-root key at a memory location corresponding to the other one of the first and second super-root keys, the first, second, and third super-root keys when stored in the memory circuit being accessible only by the program code and being modifiable only by the program code for all

modifications excluding erasure, wherein the first, second, and third super-root keys are private keys; and

a super-root key request generator for generating a super-root key request in dependence on a super-root key status.

22. (Previously Presented) The secure module according to claim 21 wherein the code executable on the encryption processor accesses the super-root keys stored in the memory circuit only in response to a request from a corresponding secure module.

23. (Previously Presented) The secure module according to claim 22 wherein the code executable on the encryption processor is for performing encryption functions the results of which are inaccessible outside of the module.

24. (Previously Presented) The secure module according to claim 23 wherein the memory circuit for storing the super-root keys is a non-volatile reprogrammable memory circuit.

25. (Previously Presented) The secure module according to claim 23 wherein the memory circuit for storing the super-root keys is one of an electrically erasable programmable read-only memory (EEPROM) circuit and a random access memory (RAM) circuit having an on-board power supply in the form of a battery.

26. (Previously Presented) The secure module according to claim 25 wherein the module is FPS140 compliant.

27. (Previously Presented) The secure module according to claim 26 wherein the module includes a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

28-32. Canceled

33. (Previously Presented) The method of claim 10 wherein the first, third, and fourth super-root keys are only for decrypting at least one of encrypted private root keys and encrypted private super-root keys generated by the key provider system.